I CLAIM:

1. An apparatus capable of detecting and preventing a plurality of rate based and non rate based denial of service attacks, said apparatus comprising:

a media access controller (MAC) interface;

a classification means operatively coupled to said MAC interface for classifying data packets received from said MAC interface according to Layer 2, Layer 3, and Layer 4 classifications, said classification means being capable of enforcing Layer 2, Layer 3, and Layer 4 accepted header syntax;

a meter means operatively coupled to said classification means, said meter means having a plurality of meters and being capable of maintaining statistics of said attacks and determining whether a threshold has been reached;

a decision multiplexer means operatively coupled to said meter means, said decision multiplexer means being capable of accepting decisions from said plurality of meters and informing a single decision to said MAC interface; and

an ager means capable of timing out flood states identified by said classification means or by said meter means, said ager means comprising

a continuous learning mechanism for continuously learning and updating said statistics.

2. The apparatus of claim 1, wherein said plurality of meters detect and prevent rate based denial of service attacks selected from the group consisting of synchronization (SYN) flood, Transmission Control Protocol (TCP) flood, Internet Control and Message Protocol (ICMP) flood, User Datagram Protocol (UDP) flood, port scan, source flood, destination

flood, broadcast flood, Address Resolution Protocol (ARP) flood, Reverse ARP (RARP) flood, multicast flood, Virtual Local Area Network (VLAN) flood, double encapsulated VLAN flood, protocol flood, Internet Protocol (IP) option flood, fragment flood, port flood, Layer 2 floods, Layer 3 floods, and Layer 4 floods.

3. The apparatus of claim 2, wherein said rate based denial of service attacks are to an end node or from said end node to other nodes on the internet.

4. The apparatus of claim 1, further comprising:

a SYN flood detection and prevention mechanism having a support means for creating a plurality of legitimate IP addresses during normal operation when the TCP state transitions to ESTABLISHED.

5. The apparatus of claim 4, wherein said SYN flood detection and prevention mechanism allows only said plurality of legitimate IP addresses to be stored during normal operation.

6. The apparatus of claim 5, further comprising:

a zombie flood detection and prevention mechanism having

a means for limiting connections to said plurality of legitimate IP addresses stored during normal operation; and

a means for determining a threshold for said connections based on baseline traffic learned during normal operation.

7. The apparatus of claim 1, further comprising:

a source tracking mechanism multiplicatively incrementing count for sources that send identified flood data, thereby distinguishing said sources from others that send non-flood data.

8. The apparatus of claim 1, wherein said ager means collects continuous learning data for different network characteristics.

9. The apparatus of claim 8, wherein said plurality of meters identify whether a threshold of counts for a particular network characteristic has been reached.

10. The apparatus of claim 9, wherein said threshold has been reached and said plurality of meters inform said decision multiplexer means to block traffic with said particular network characteristic for a certain time period.

11. A system for detecting and preventing rate based and non rate based denial of service attacks, said system comprising:

a host having a threshold estimation mechanism for estimating traffic thresholds based on past traffic, baseline, trend, and seasonality; and

an intrusion prevention apparatus operatively coupled to said host, said intrusion prevention apparatus comprising:

an intrusion prevention logic; and

computer executable instructions controlling said intrusion prevention logic, wherein said intrusion prevention logic comprises:

a media access controller (MAC) interface;

a classification means operatively coupled to said MAC interface for classifying data packets received from said MAC interface according to Layer 2, Layer 3, and Layer 4 classifications, said classification means being capable of enforcing Layer 2, Layer 3, and Layer 4 accepted header syntax;

a meter means operatively coupled to said classification means, said meter means having a plurality of meters and being capable of maintaining statistics of said attacks and determining whether a threshold has been reached;

a decision multiplexer means operatively coupled to said meter means, said decision multiplexer means being capable of accepting decisions from said plurality of meters and informing a single decision to said MAC interface; and

an ager means capable of timing out flood states identified by said classification means or by said meter means, said ager means comprising

a continuous learning mechanism for continuously learning and updating said statistics.

12. The system of claim 11, wherein said plurality of meters detect and prevent rate based denial of service attacks selected from the group consisting of synchronization (SYN) flood, Transmission Control Protocol (TCP) flood, Internet Control and Message Protocol (ICMP) flood, User Datagram Protocol (UDP) flood, port scan, source flood, destination flood, broadcast flood, Address Resolution Protocol (ARP) flood, Reverse ARP (RARP) flood, multicast flood, Virtual Local Area Network (VLAN) flood, double encapsulated VLAN

flood, protocol flood, Internet Protocol (IP) option flood, fragment flood, port flood, Layer 2 floods, Layer 3 floods, and Layer 4 floods.

13. The system of claim 12, wherein said rate based denial of service attacks are to an end node or from said end node to other nodes on the internet.

14. The system of claim 11, further comprising:

a SYN flood detection and prevention mechanism having a support means for creating a plurality of legitimate IP addresses during normal operation when the TCP state transitions to ESTABLISHED.

15. The system of claim 14, wherein said SYN flood detection and prevention mechanism allows only said plurality of legitimate IP addresses to be stored during normal operation.

16. The system of claim 15, further comprising:

a zombie flood detection and prevention mechanism having

a means for limiting connections to said plurality of legitimate IP addresses stored during normal operation; and

a means for determining a threshold for said connections based on baseline traffic learned during normal operation.

17. The system of claim 11, further comprising:

a source tracking mechanism multiplicatively incrementing count for sources that send identified flood data, thereby

distinguishing said sources from others that send non-flood data.

18. The system of claim 11, wherein said ager means collects continuous learning data for different network characteristics, wherein said plurality of meters determines whether to block traffic with a particular network characteristic for a certain time period.

19. The system of claim 18, wherein said threshold estimation mechanism further comprises:

a means for producing traffic forecast for said network characteristics; and

a means for determining said traffic thresholds and a deviation of said traffic forecast.

20. The system of claim 18, wherein said particular network characteristic is a destination port.